REMARKS

Claims 1-3, 5-12, 14-21, and 23-26 are currently pending.

CLAIMS REJECTIONS UNDER 35 U.S.C. § 102

Claims 1-3, 5-12, 14-21, and 23-26 have been rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Pat. No. 5,286,007, issued to Sakaki, et al. (hereinafter *Sakaki*). Applicants respectfully traverse the foregoing rejections for the following reasons.

Regarding the grounds for rejecting claim 1, the Office Action asserts on page 3, reference item 8, that *Sakaki* discloses an enable flag (Fig. 2, bit S1) being used to control access to a device (memory devices 12 and 17 in Figs. 1 and 2; col. 5, lines 24-33), and further discloses a persistent enable flag that is write-accessible only in response to a detected power-on reset (col. 3, lines 21-40 and col. 4, lines 49-56, Fig. 1, bit S2; col. 5, line 34 – col. 6, line 7), wherein the persistent enable flag is read-only accessible to runtime program instructions (col. 4, lines 43-56).

Sakaki describes S1 and S2 as two constituent bits of a single "security flag." Applicants contend that the S1 and S2 bits disclosed by *Sakaki* do not share the functional characteristics of the "persistent enable flag" and "pending state change flag" recited in Applicants' claim 1. The S1 and S2 bits constitute a single security flag that is monitored by a security flag monitor circuit 25 which reads the two-bit flag when receiving a power-on reset signal and provides a recognition result to a bus line control circuit (see col. 4, lines 42-61, and col. 5, lines 15-33). Nothing in the description of the two-bit security flag consisting of bits S1 and S2 or elsewhere does *Sakaki* disclose a persistent enable flag that is "write-accessible only in response to a detected power-on reset" and is "read-only accessible to runtime program instructions" as recited in Applicants' claim 1. Furthermore, *Sakaki* does not disclose an access control system including the foregoing persistent enable flag and further including a pending state change flag for setting an intended next state of the persistent enable flag and that, unlike the persistent enable flag, is write-accessible by runtime program instructions. In fact, *Sakaki* includes no disclosure or suggestion that the flag bits S1 and S2 are functionally distinct in terms of protection/accessibility (i.e. write-only accessible versus read-only accessible to runtime program instruction; write-accessible only in response to a detected power-on reset).

Regarding the grounds for rejecting independent claims 9 and 18, the Office Action asserts in reference item 13 on pages 4-5, that *Sakaki* substantially discloses the setting/resetting of persistent and pending flags executed through runtime instructions (col. 5, lines 21-30; col. 4, lines 58-65; and col. 5, lines 43-47). At col. 4, lines 58-61, *Sakaki* discloses the general concept of reading a security flag coincident to receiving a power-on reset signal. However, neither in the foregoing passages nor elsewhere does *Sakaki* disclose or suggest a step of, in response to a power-on reset cycle, determining the state of a pending state change flag that is accessible by runtime programs to set an intended next state of a persistent enable flag that enables or disables access to the device and setting or resetting the persistent enable flag in accordance with the state of the pending state flag.

Since *Sakaki* does not teach each feature recited by Applicants' claims, Applicants respectfully request withdrawal of the present claim rejections and issuance of a Notice of Allowance for all claims now pending. Applicants urge the Examiner to contact the undersigned representative of record at 512.343.6116 if such would further or expedite the prosecution of the present Application.

Respectfully submitted,

Matthew W. Baca
Reg. No. 42,277
Dillon & Yudell LLP
8911 North Capital of Texas Highway
Suite 2110
Austin, Texas 78759
512.343.6116

ATTORNEY FOR APPLICANT(S)